

## Browser Settings for Safe Web Surfing

There are steps you can easily take to make sure your web browsing doesn't expose you to too many malicious activities. By modifying some simple settings in your web browser, you can limit what web servers attempt to do with your computer.

The **Firefox** web browser is targeted much less often than Microsoft's Internet Explorer for security vulnerabilities. For this reason alone it's a good idea to use Firefox as your main browser, but Firefox and Internet Explorer still need to be properly configured to protect you from harmful web sites.



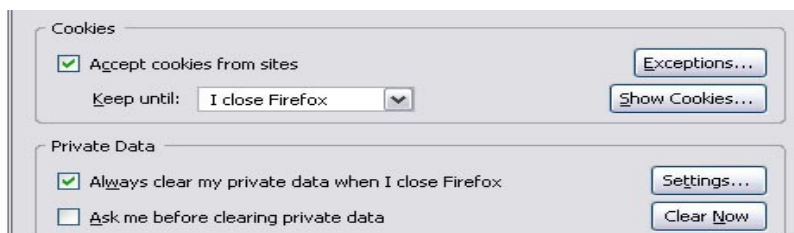
In Firefox, open the Options menu from the Tools drop-down tool-bar. Select the Security tab, and ensure the **top two check-boxes** are checked. This will block websites from automatically installing software into your browser, and will also check the sites you visit against a list of known malicious sites.

Under the Content tab in the Options window, take a look at the top check boxes. Pop-up windows are often annoying, but are also used by malicious websites to serve up bad content or entice you to surf somewhere that may be unsafe.

**JavaScript** is a scripting language that enables some interactivity on websites, but can also be used to modify your browsers behavior and appearance. Although you may not want to completely disable JavaScript, examine the Exceptions menu and clear the check boxes for the activities you don't want JavaScript to perform on your PC.



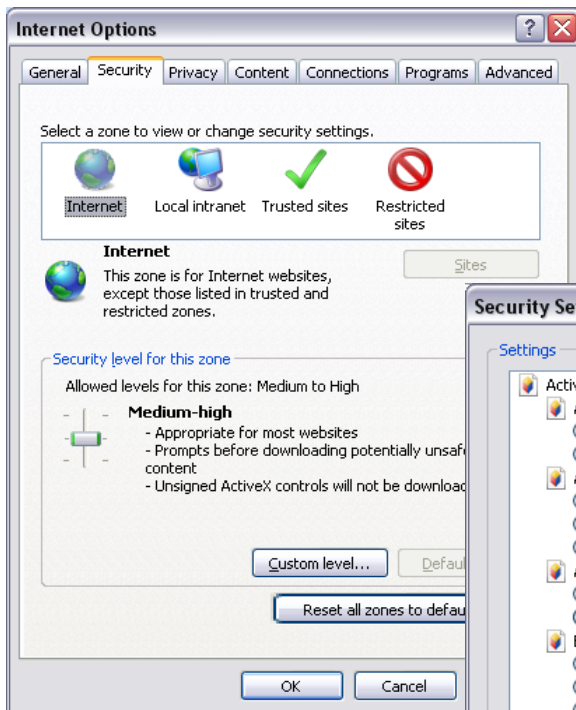
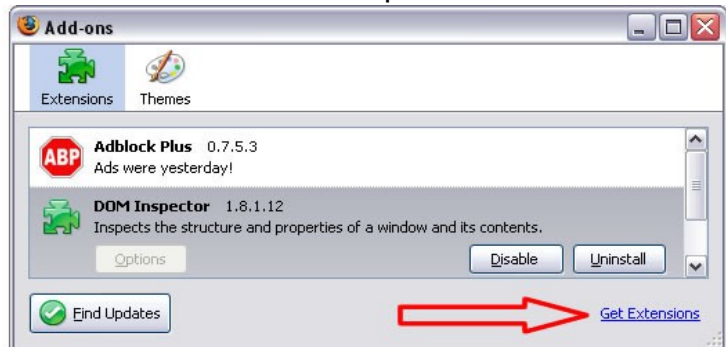
Finally, under the Privacy options tab, consider clearing your **cookies** every time you close Firefox. This will result in having to log back into web-based email or other account-driven sites every time you visit them, but will help protect your privacy by removing cookies that



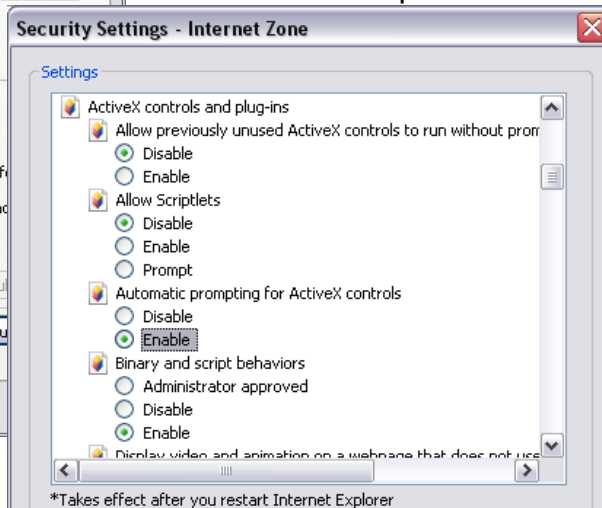
track your browsing history and report information about you back to certain web servers. Examine the Private Data settings for additional information you'd like Firefox to remove when you're done surfing.

Additionally, Firefox offers a number of browser plug-ins that help protect you from unwanted content and malicious activity. Use the Tools -> Add-Ons menu to explore what add-ons are available for use.

The [Netcraft toolbar](#) is an excellent add-on to help you identify if a malicious website is masquerading as a legitimate site, as does the [Phish Tank](#) add-on. Also, the [Adblock Plus](#) extension is excellent at blocking advertising (both static and Flash-enabled) that may entice you to a malicious site. The [No Script](#) add-on allows you to define which sites are allowed to run scripts in your web browser, and [Safe Cache](#) keeps your temporary Internet files segmented so websites can't determine your browsing history by looking through your cached files.



If you prefer to use Internet Explorer, make sure you've upgraded to the newest version that Microsoft offers, and have applied all patches available from the Microsoft Update website. Internet Explorer offers similar security and privacy measures in the Internet Options window, found under the Tools drop-down menu.

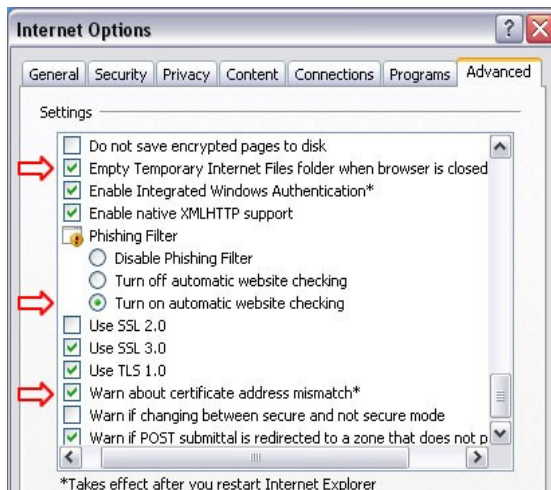


The slider for the Internet Zone under the security tab and the slider on the Privacy tab should be set to no lower than a medium level. This will help protect you on the Internet while using Internet Explorer.

If you click the Custom Level button below the security slider, you'll be presented with a large amount of additional security settings. One set of setting to pay attention to are the ActiveX

controls. A number of security vulnerabilities are associated with these types of interactive controls. Changing the security slider will automatically change these settings, so ensure they're set properly to disallow all but necessary activity. You can also find options here to control the behavior of JavaScript, as we did earlier in the Firefox browser.

More important security and privacy settings are found under the Advanced tab. Scroll to the bottom of the list and you'll find a number of settings you may want to modify.



You can direct IE to empty your temporary Internet files (also known as your browser's cache) every time you exit. Also, enable the automatic Phishing Filter – this is similar to the functionality in Firefox that checks if a website is a forgery.

Phishing is a method used by Internet scammers to steal personal information by pretending to be a website you would otherwise trust.

**For more information on secure browsing, Internet security, and Linux and Mac-based security, contact VeriSpect Security Services and Consulting – we're experts on securing your data and can create a custom security plan to fit your needs and your budget. More information at [www.Verispect.net](http://www.Verispect.net) or through email at [info @ verispect.net](mailto:info@verispect.net).**

